REMARKS/ARGUMENTS

The present Amendment is in response to the Final Office Action having a mailing date of April 28, 2006. Claims 1-22 are pending in the present Application. Applicant has amended claims 5 and 13. Consequently, claims 1-22 remain pending in the present Application.

This application is under Final Rejection. Applicant has presented arguments hereinbelow that Applicant believes should render the claims allowable. In the event, however, that the Examiner is not persuaded by Applicant's arguments, Applicant respectfully requests that the Examiner enter the Amendment to clarify issues upon appeal.

Applicant has amended claims 5 and 13 to correct an error. In particular, claims 5 and 13 have been amended to recite a user level key pair and an encryption level key pair in lieu of a double recitation of the encryption level key pair. Support for the amendment can be found in the specification, page 2, line 20-page 3, line 23. Thus, claims 5 and 13 recite, as the Examiner has assumed, a hardware key pair level, a platform key pair level, an encryption key pair level, and a user key pair level. Applicant respectfully submits that no new matter is added and no new search is required.

In the above-identified Office Action, the Examiner rejected claims 5 and 13 under 35 U.S.C. § 112, second paragraph. In particular, claims 5 and 13 previously recited "an encryption key pair level and an encryption key pair level."

Applicant respectfully traverses the Examiner's rejection. Claims 5 and 13 currently recite "an encryption key pair level and a user key pair level." Thus, claims 5 and 13 no longer contain a double recitation of the encryption key pair level. Moreover, claim 13 has been harmonized with claim 15. Accordingly, Applicant respectfully submits that claims 5 and 13 are clear and definite.

In the above-identified Office Action, the Examiner rejected claims 1-22 under 35 U.S.C. § 102 as being anticipated by U.S. Patent 6,446,209 (Kern).

Applicant respectfully disagrees with the Examiner's rejection. Claim 1 recites a method for control of key pair usage in a computer system. The method recited in claim 1 includes creating key pair material for utilization with an embedded security chip of the computer system. The key pair material is specifically recited as including tag data. Claim 1 further recites determining whether the key pair material is bound to the embedded security chip based on the tag data. Claim 7 recites an analogous computer system including a main processor and a security processor. The security processor stores tag data with key pair material and determines binding of the key pair material to the security processor based on the tag data. Similarly, claim 16 recites a method for controlling usage of key pairs in a hierarchical structure of key pairs in an embedded security chip. Claim 16 recites storing tag data with key pair data for each level of the hierarchical structure and determining whether the key pair data is bound to the embedded security chip based on the tag data.

Thus, claims 1, 7, and 16 recite the use of an embedded security chip/processor, with which the key pair material is used. In particular, the binding status of the key pair is determined by the embedded security chip/processor. The embedded security chip/processor does so based on the tag data corresponding to the key pair material. Consequently, a user can either be bound to a particular system or may be verified securely on any system. Specification, page 7, lines 9-13. Moreover, as described in the specification, an embedded security chip/processor is one which is embedded on the system board of the computer system and coupled to a separate, main processor. Specification, page 1, lines 15-20 and FIG. 1. Using this embedded security processor, tag data can be stored and evaluated to determine the binding of key pair material to the security processor.

Although Kern functions for its intended purpose, Kern fails to teach or suggest the methods and system recited in claims 1, 7, and 16. In particular, Kern fails to teach or suggest utilizing key pair material for use with an embedded security chip, or security processor, in conjunction with the recited tag data, using the recited tag data to determine binding, or the use of key pairs.

Kern describes a storage controller that selectively allows access to a corresponding storage device based on a key. Kern, Abstract, lines 1-5. The storage controller of Kern allows the storage device to be directly attached to a network without the use of an intermediate server to perform security functions. Kern, Abstract, lines 7-10 and col. 2, lines 36-42. Kern specifically describes the components of this controller as including an interface 120, a security module 122, and a storage map. Kern, FIG. 1A; col. 6, lines 47-51; and col. 6, line 66-col. 7, line 1. An example of the storage map, which includes an identification of the storage region, a reference key (of "1", "2", or "none") and a security type, is in Table 1 of Kern. Despite a detailed discussion of the security controller, Applicant has found no mention in Kern of the security module 122 residing on the system board along with a separate processor. Instead, the security module of Kern apparently is the only processor for the security controller. Thus, apparently all of the functions of the security controller, whether related to security or not, would be performed by the security module. For example, Kern describes the security controller as performing a variety of storage-related functions in addition to security. Kern, col. 5, lines 16-23. The security module of the security controller would apparently perform these functions. Thus, there is apparently no separate, dedicated embedded security processor on a system board along with an additional processor. Consequently, Kern fails to teach or suggest the use of the recited embedded security processor.

Kern also fails to teach or suggest the recited tag data. The Examiner cited Kern, col. 11, lines 8-10 as teaching the key pair material including the recited tag data. Applicant respectfully disagrees with the Examiner. The cited portion of Kern merely describes one type of security that may be provided. In whole, this portion of Kern states:

> In step **406**, the application program **110-112** chooses a desired level of security for the region to be allocated. In this example, the levels of security, also called "security types" or "access levels" include:
>
> 1) "read/write protect" where both Reads and Writes are prohibited. Here, the storage controller **106** prevents reading and writing to the associated storage regions unless the host presents an appropriate key.
> 2) "write protect" where Writes are prohibited but Reads permitted. Here, as discussed in greater detail below, the controller **106** will prevent hosts from writing the storage region unless the host presents an appropriate key. The associated storage region may be freely read.
> 3) "none" or "no security," where any host can read and write to this storage region without presenting a key. As an example, "none" may be used as a default value if another security type is not chosen.

Kern, col. 10, line 62-col. 11, line 11. Consequently, this portion of Kern merely notes different types of security levels to which the key may correspond. Even Table 1 of Kern merely mentions security keys, storage regions, and the type of security. The references in Table 1 of Kern to the reference security key merely restate the security type and correspond to the three types of security or access levels. Thus, neither the cited portion of Kern nor Table 1 indicates that a key pair material includes tag data. Moreover, a search of Kern fails to turn up the term "tag" associated with the key of Kern. Because Kern fails to describe the recited tag data, Kern must also fail to determine binding based upon the tag data. Consequently, Kern fails to teach or suggest the recited tag data and determining binding based upon the tag data.

Kern also fails to describe the recited key pair material. As described in the specification, a key pair includes two keys for each level. Specification, page 2, lines 22-23. In contrast, Applicant can find no mention in Kern of using key pairs. Instead, a simple key, or password, is apparently used to access the data in the storage that is managed by Kern's storage controller. Kern, col. 6, lines 56-65. Consequently, Kern also fails to describe the recited key pair material. Accordingly, for at least the above-identified reasons, Applicant respectfully submits that claims 1, 7, and 16 are allowable over the cited references.

Claims 2-6 and 20 depend upon independent claim 1. Claims 8-15 and 21 depend upon independent claim 7. Consequently, the arguments herein with respect to claims 1 and 7 apply with full force to claims 2-6, 8-15 and 20-21. Claims 17-19 and 22 depend upon claim 16. Consequently, the arguments herein with respect to claim 16 apply with full force to claims 17-19 and 22. Accordingly, Applicant respectfully submits that claims 2-6, 8-15, and 17-22 are allowable over the cited references.

Applicant's attorney believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicant's attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

June 28, 2006
Date

Janyce R. Mitchell
Attorney for Applicant(s)
Reg. No. 40,095
(650) 493-4540